



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/596,003

02/08/2007

Maria Pilar Gonzalez Lopez

P18126-US1

1612

27045

7590

12/04/2009

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER

KATSIKIS, KOSTAS J

ART UNIT

PAPER NUMBER

2441

MAIL DATE

DELIVERY MODE

12/04/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/596,003	Applicant(s) GONZALEZ LOPEZ ET AL.	
	Examiner Kostas Katsikis	Art Unit 2441	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 September 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 37-72 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 37-72 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office Action is in response to the Amendment filed on September 14, 2009, in which claims 42-45, 53-56, 62, and 64-67 have been amended. Accordingly, claims 37-72 remain pending for examination.

Status of Claims

2. Claims 37-72 are pending, of which claims 37-72 are rejected under 35 U.S.C. 103.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 37-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black et al. (United States Patent Application Publication No. US**

2002/0116485 A1), hereinafter “Black” in view of Esko Freese (International Patent Application Publication No. WO 02/19116 A2), hereinafter “Freese”.

Regarding claims 37, 51, and 62, **Black** discloses an apparatus for mediating in management orders between a plurality of origin managers and a plurality of managed devices in a telecommunications system, the management orders intended to execute management operations over the managed devices, comprising:

a communication receiver component arranged to receive a management order from an origin manager (*wherein templates may be originated in OSS client and relayed to and received in NMS servers*) (**Black, FIG. 3b and 3h-3i combined, paragraphs [0408]-[0416]**);

a management access template, the management access template being one selected from the group consisting of: a first management access template in relationship with an identifier of the origin manager (*wherein network manager may need to supply username and password upon establishing connection with OSS client, NMS server, and corresponding network device*) (**Black, FIG. 3i, paragraphs [0415]-[0416]**); a second management access template in relationship with an identifier of a managed data object affected by the management order (*wherein flexible naming procedure is used to derive and identify objects with which processes need to communicate with*) (**Black, FIG. 1, paragraph [0442]**); and a third management access template in relationship with an identifier of a managed device affected by the management order (*wherein IP address and/or (DNS) name is provided for host lookup*

Art Unit: 2441

used to determine IP address for accessing corresponding network device) (**Black, FIG. 3i, paragraphs [0415]-[0416]**); and

a communication sender component arranged to send an allowed management order to a managed device (*wherein NMS server relays template with instructions to corresponding network device*) (**Black, FIG. 3b and 3h-3i combined, paragraphs [0408]-[0416]**).

Black does not explicitly disclose a management verifier component arranged to determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute.

However **Freese** discloses a management verifier component arranged to determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute (*wherein operator initiates sending of instruction from originating management console, containing identity of application to be controlled, and is cryptographically signed for authentication*) (**Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**).

Black and **Freese** are analogous art because they are from the same problem solving area, namely, management of client devices in telecommunications networks.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Black** and **Freese** before him or her, to modify the telecommunications management apparatus of **Black**, to include the cryptographic-authenticating-instruction functionality of **Freese**, with reasonable expectation that this would result in a system that guaranteed the security and reliability of received

Art Unit: 2441

management instructions, without the requirement of special secure network management protocols such as SNMP Version 3, thereby allowing any compatible network management protocol to be used and not a specially enhanced version having built-in encryption and security. This approach to improving the telecommunications management apparatus of **Black** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Freese**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Black** and **Freese** to obtain the invention as specified in claim 37.

Claim 62 includes a computer program for performing the limitations substantially as described in claim 37. **Black-Freese** discloses a computer program for mediating from a computer-based apparatus in management orders between a plurality of origin managers and a plurality of managed devices in a telecommunications system for performing the limitations substantially as described in claim 37 (*wherein computer system in telecommunications network with plurality of origin managers and plurality of managed devices includes centralized processor with control processor subsystem that executes instance of the kernel including master control and server programs to actively control system operation by performing major portion of control functions*) (**Black, FIG. 1, and FIG. 2a-2b, paragraphs [0103]-[0110], [0112]-[0118], and [0125]-[0126]**). The motivation regarding the obviousness of claim 37 is also applied to claim 62; therefore, claim 62 is rejected under the same rationale.

Additionally, claim 51 recites a method for mediating in the management of a

Art Unit: 2441

plurality of devices from a plurality of origin managers that performs the limitations substantially as described in claims 37 and 62 and is rejected for similar reasons.

Regarding claim 38, **Black-Freese** discloses the apparatus of claim 37, wherein the first management access template further comprises at least one access attribute selected from the group consisting of: an identifier of an allowed management operation (*wherein instruction is identified with cryptographic signature*) (**Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**); an identifier of an allowed managed data object; a pattern structure of the managed data object; an identifier of an allowed managed device; an identifier of an allowed management operation over an allowed managed device; and an identifier of an allowed management operation over an allowed managed data object. The motivation regarding the obviousness of claim 37 is also applied to claim 38.

Regarding claim 39, **Black-Freese** discloses the apparatus of claim 37, wherein the second management access template further comprises at least one access attribute selected from the group consisting of: a pattern structure of the managed data object; an identifier of an allowed management operation (*wherein instruction is identified with cryptographic signature*) (**Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**); an identifier of a managed device holding the managed data object; an identifier of an allowed origin manager; an identifier of an allowed management operation from an allowed origin manager; and an identifier of an allowed management operation over a

Art Unit: 2441

holding managed device. The motivation regarding the obviousness of claim 37 is also applied to claim 39.

Regarding claim 40, **Black-Freese** discloses the apparatus of claim 37, wherein the third management access template comprises at least one access attribute selected from the group consisting of: an identifier of an allowed management operation (*wherein instruction is identified with cryptographic signature*) (**Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**); an identifier of a managed data object held on the managed device; an identifier of an allowed origin manager; an identifier of an allowed management operation from an allowed origin manager; and an identifier of an allowed management operation over a held managed data object. The motivation regarding the obviousness of claim 37 is also applied to claim 40.

Regarding claim 41, **Black-Freese** discloses the apparatus of claim 37, wherein the management verifier component is arranged to determine, from the identifier of a management operation, at least one identifier, the identifier being one selected from the group consisting of: an identifier of a managed data object affected by the operation; and an identifier of a managed device, affected by the operation (*wherein the header of the SMS message contains the phone number identifying the device affected by the operation*) (**Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**). The motivation regarding the obviousness of claim 37 is also applied to claim 41.

Regarding claim 42, **Black-Freese** discloses the apparatus of claim 37, wherein the management verifier component is arranged to select a management access template, among the first second and third management templates, according to an identifier received in a management order (*wherein a number of various management templates may be transmitted to NMS server from OSS client, templates with instructions may be selected after verified via verification component*) (**Black, FIG. 3b and 3h-3i combined, paragraphs [0408]-[0416], Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**). The motivation regarding the obviousness of claim 37 is also applied to claim 42.

Regarding claim 43, **Black-Freese** discloses the apparatus of claim 42, wherein the management verifier component is arranged to select a management access template, among the first second and third management templates, according to an access attribute comprised in another selected management access template (*wherein template may be selected and verified based on identification of authorized cryptographic signature, which is comprised in other templates*) (**Black, FIG. 3b and 3h-3i combined, paragraphs [0408]-[0416], Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**). The motivation regarding the obviousness of claim 37 is also applied to claim 43.

Regarding claim 44, **Black-Freese** discloses the apparatus of claim 42, wherein the identifier (ORID) of an origin manager comprises at least one identifier selected from

Art Unit: 2441

the group consisting of: an identifier of a management server sending a management order; and an identifier of a user operating the management server (*wherein network manager may need to supply username and password upon establishing connection with OSS client, NMS server, and corresponding network device*) (**Black, FIG. 3i, paragraphs [0415]-[0416]**); and

wherein the management verifier component is arranged to select the first management access template according to the at least one identifier (*wherein verifier selects management instructions upon verifying cryptographic signature*) (**Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**). The motivation regarding the obviousness of claim 37 is also applied to claim 44.

Regarding claim 45, **Black-Freese** discloses the apparatus of claim 42, wherein the identifier (ORID) of an origin manager comprises at least one identifier selected from the group consisting of: an identifier of a management server sending a management order; and an identifier of a user operating the management server (*wherein network manager may need to supply username and password upon establishing connection with OSS client, NMS server, and corresponding network device*) (**Black, FIG. 3i, paragraphs [0415]-[0416]**); and wherein the management verifier component is arranged to authenticate the at least one identifier (*wherein verifier selects management instructions upon verifying cryptographic signature*) (**Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**). The motivation regarding the obviousness of claim 37 is also

Art Unit: 2441

applied to claim 45.

Regarding claim 46, **Black-Freese** discloses the apparatus of claim 42, wherein the management verifier component is arranged to determine a management role associated to at least one identifier, the identifier being one selected from the group consisting of: an identifier of a management server sending a management order; and an identifier of a user operating the management server (*wherein network manager may need to supply username and password upon establishing connection with OSS client, NMS server, and corresponding network device*) (**Black, FIG. 3i, paragraphs [0415]-[0416]**). The motivation regarding the obviousness of claim 37 is also applied to claim 46.

Regarding claim 47, **Black-Freese** discloses the apparatus of claim 46, wherein the management verifier component is further arranged to select at least one management access template in relationship with the role (*wherein network manager may need to supply username and password upon establishing connection with OSS client, NMS server, and corresponding network device, verifier selects management instructions upon verifying cryptographic signature*) (**Black, FIG. 3i, paragraphs [0415]-[0416], Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**). The motivation regarding the obviousness of claim 37 is also applied to claim 47.

Regarding claim 48, **Black-Freese** discloses the apparatus of claim 46, wherein at least one management access template among the second or third management templates comprises an identifier (ROm) of at least one role as an access attribute, and wherein the Management Verifier Component is further arranged to check whether the management order fits with the role (*wherein batch templates may contain names of control templates to cause OSS client to issue calls to NMS server affecting corresponding network device, authorized network manager non-interactively completing provisioning tasks and building custom services*) (**Black, FIG. 3b, paragraphs [0410]-[0411]**). The motivation regarding the obviousness of claim 37 is also applied to claim 48.

Regarding claim 49, **Black-Freese** discloses the apparatus of claim 37, wherein the management verifier component is arranged to determine whether a managed data object affected by an allowed management order is an access attribute in a management access template, and further comprising a management execution component, arranged to execute a management operation over the access attribute (*wherein templates comprise various parameter values which affect data objects, may be provisioned by network managers upon establishing connections with NMS server and network devices, while verifier component verifies and determines whether object is known attribute, (i.e., antivirus signatures previously identified and stored in database, used to identify viruses in scanned data), upon authentication, management agent may update signature database and execute instruction*) (**Freese, FIG. 1-2, page 6, lines**

Art Unit: 2441

17-26). The motivation regarding the obviousness of claim 37 is also applied to claim 49.

Regarding claim 50, **Black-Freese** discloses the apparatus of claim 37, wherein the communication receiver component is further arranged to receive an access request from an origin manager (*wherein NMS server issues provisioning requests for template in response to calls from OSS client*) (**Black, FIG. 3h, paragraph [0414]**);

wherein the management verifier component is further arranged to determine the first management access template (*wherein verifier component determines whether instruction is authorized*) (**Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**); and

wherein the communication sender component is further arranged to send an access response to the origin manager that comprises an access attribute of the management access template (*wherein network manger may send command to interactive interpreter to cause OSS client to display available and acceptable parameter values for each template*) (**Black, FIG. 3i, paragraphs [0417]-[0418]**). The motivation regarding the obviousness of claim 37 is also applied to claim 50.

Claims 52-61 are corresponding method claims of apparatus claims 41-50; therefore, they rejected under the same rationale.

Claims 63-72 are corresponding computer program claims of apparatus claims 41-50; therefore, they are rejected under the same rationale.

Response to Arguments

5. Applicant's arguments, see page 14, filed September 14, 2009, with respect to Objections to the Abstract have been fully considered and are persuasive. The Objections to the Abstract as set forth in the previous Office Action have been withdrawn.

6. Applicant's arguments, see pages 15, filed September 14, 2009, with respect to Objections to the Specification have been fully considered and are persuasive. The Objections to the Specification as set forth in the previous Office Action have been withdrawn.

7. Applicant's arguments, see page 15, filed September 14, 2009, with respect to Claim Objections have been fully considered and are persuasive. The Objections to Claims 42-43, 53-54, and 64-65 as set forth in the previous Office Action have been withdrawn.

8. Applicant's arguments, see page 15, filed September 14, 2009, with respect to Claim Rejections under 35 U.S.C. § 112, second paragraph have been fully considered

Art Unit: 2441

and are persuasive. The Rejections to Claims 43-45, 54-56, and 65-67 as set forth in the previous Office Action have been withdrawn.

9. Applicant's arguments, see pages 15-16, filed September 14, 2009, with respect to Claim Rejections under 35 U.S.C. § 101 have been fully considered and are persuasive. The Rejections to Claims 65-72 as set forth in the previous Office Action have been withdrawn.

10. Applicant's arguments, see pages 14-15, filed September 14, 2009, with respect to Rejections of Claims 37-72 under 35 U.S.C. § 103(a) have been fully considered but they are not persuasive.

11. In the Remarks, Applicant argued in substance that

(A) Applicant argued on pages 16-17 of the Remarks, the claimed apparatus's configuration where it is located between origin managers and managed devices and the claimed apparatus's mediation of management orders are not taught or suggested by the Examiner's closest prior art **Black (Recited from pages 16-17 of Remarks)**. **Black** does not disclose any device that reads-on the claimed apparatus which is in a position to mediate management orders between a plurality of origin managers and a plurality of managed devices. Thus, **Black** does not disclose or suggest anything related to the claimed apparatus which mediates management orders received from

Art Unit: 2441

origin managers before sending allowed management orders to the managed devices

(Recited from page 17 of Remarks).

As to point **(A)**, Examiner respectfully disagrees, noting that there is nothing in the claim language that suggests that the claimed apparatus *is located between origin managers and managed devices*. The preamble of **Claim 37** recites,

Apparatus for mediating in management orders between a plurality of origin managers and a plurality of managed devices in a telecommunications system, the management orders intended to execute management operations over the managed devices, comprising:

In interpreting the language of the preamble as broad as reasonably possible, Examiner respectfully submits that an apparatus is being claimed, for the functionality of mediating management orders between origin managers and managed devices. Examiner respectfully submits that there is nothing suggestive in the preamble, or in any of the limitations for that matter, of the location of the apparatus to be between the origin managers and managed devices. **Black** discloses Operation Support Services clients receiving commands for mediating in management information from a manager or network administrator, and passing the commands to the Network Management System servers **(See Black, paragraphs [408]-[416])**. Thus, Examiner respectfully submits that **Black** does disclose the claimed apparatus which is in a position to mediate management orders between a plurality of origin managers and a plurality of managed devices.

Furthermore, in response to Applicant's arguments, a recitation to the effect of the location of the claimed apparatus to be between the origin managers and the managed devices would not be given patentable weight if it were to occur in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). In this case, the apparatus would still be able to mediate management information to managed devices, from origin managers, regardless of its spatial location.

(B) Applicant argued on pages 18-19 of the Remarks, The Examiner stated that **Black** does not explicitly disclose a management verifier component arranged to determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute. This is correct, but the Examiner failed to take into account that the claimed management verifier component is arranged to determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute comprised in a management access template (**Recited from pages 18 of Remarks**). Applicant fails to see how the Examiner can indicate that **Black** does not teach a main feature (namely the management verifier component) of the present

Art Unit: 2441

invention but then contend that **Black** does teach the main feature's secondary aspects (namely the management access template). In fact, the Examiner's logic indicates that they had to use some sort of improper hindsight in an attempt to contend that **Black** taught the claimed invention (**Recited from page 18 of Remarks**). Applicant submits that **Freese** is not related whatsoever to the claimed apparatus or the claimed management verifier component (**Recited from page 19 of Remarks**).

As to point **(B)**, Examiner respectfully disagrees, noting that in response to applicant's argument that the Examiner failed to take into account that the claimed management verifier component is arranged to determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute comprised in a management access template, and that **Black** does not teach a main feature (namely the management verifier component) of the present invention but then contend that **Black** does teach the main feature's secondary aspects (namely the management access template), Examiner respectfully submits that applicant's remarks are misplaced.

In this case, the secondary features of the claimed apparatus's verifier component are taught by **Black**:

a management access template, the management access template being one selected from the group consisting of: a first management access template in relationship with an identifier of the origin manager (*wherein network manager may need to supply username and password upon establishing connection with OSS client*,

Art Unit: 2441

NMS server, and corresponding network device) (**Black, FIG. 3i, paragraphs [0415]-[0416]**); a second management access template in relationship with an identifier of a managed data object affected by the management order (*wherein flexible naming procedure is used to derive and identify objects with which processes need to communicate with*) (**Black, FIG. 1, paragraph [0442]**); and a third management access template in relationship with an identifier of a managed device affected by the management order (*wherein IP address and/or (DNS) name is provided for host lookup used to determine IP address for accessing corresponding network device*) (**Black, FIG. 3i, paragraphs [0415]-[0416]**). However the verifier component is not taught by **Black**, But is instead found in **Freese** (*wherein operator initiates sending of instruction from originating management console, containing identity of application to be controlled, and is cryptographically signed for authentication*) (**Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9**). The verifier component does happen to be located within the managed device, but this detail is irrelevant because the cryptographic-authentication (main feature, namely management verifier component), would be used to modify the OSS client of **Black** to verify that the associated management information commands are authentic. Moreover it is well known in the art that templates exist for dynamic encryption, and it would therefore be obvious to one of ordinary skill in the art to include a dynamic encryption template for the immediate need of decoding a private key of a management instruction upon being sent, such that each management instruction were authenticated prior to being sent.

Furthermore, in response to applicant's argument that the examiner's conclusion

Art Unit: 2441

of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). Examiner respectfully submits that in the instant claim, **Freese** teaches verifying an instruction through encryption means, which is not taught by the Applicant's disclosure, though is however a technique within the level of ordinary skill at the time the claimed invention was made. Therefore, it would have been obvious to one of ordinary skill in the art to modify the telecommunications management apparatus of **Black**, to include the cryptographic-authenticating-instruction functionality of **Freese**, with reasonable expectation that this would result in a system that authenticated a management information instruction prior to being sent, as claimed in claim 37, that guaranteed the security and reliability of received management instructions, without the requirement of special secure network management protocols such as SNMP Version 3, thereby allowing any compatible network management protocol to be used and not a specially enhanced version having built-in encryption and security. **Freese** and **Black** each deal with telecommunications networks, and provisioning devices with management configuration information. Thus, Examiner respectfully submits that **Freese** is related to the claimed apparatus or the claimed management verifier

Art Unit: 2441

component.

Conclusion

12. Applicant's arguments as well as request for reconsideration filed on September 14, 2009 have been fully considered but they are not deemed to be persuasive.

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kostas Katsikis whose telephone number is (571)270-5434. The examiner can normally be reached on Monday - Friday.

Art Unit: 2441

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wing Chan can be reached on (571)272-7493. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Wing F. Chan/
Supervisory Patent Examiner, Art Unit 2441

/Kostas Katsikis/
Examiner
Art Unit 2441

December 1, 2009